TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35.U.S.C. 371	EXPRESS MAIL LABEL No **EK839858732US**	DATE 17 AUGUST 2000
	ATTORNEY'S DOCKET NO A33361 PCT USA	
	U S APPLICATION NO 09/622470	

INTERNATIONAL APPLICATION NO PCT/SG98/00023	INTERNATIONAL FILING DATE 18 MARCH 1998	PRIORITY DATE CLAIMED 18 MARCH 1998

TITLE OF INVENTION
METHOD AND APPARATUS FOR CAMOUFLAGING DATA

APPLICANT(S) FOR DO/EO/US
ANTHONY TUNG SHUEN HO

Applicant herewith submits to the United States Designated /Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(I).
4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [ ] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [ ] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:

Copy of International Publication No. WO 99/48006 (w/8 sheets drawings, 16 pages specs, 10 pages claims)
International Search Report
PCT/RO/101
PCT/IB/306
PCT/IB/332
PCT/IPEA/416
PCT/IPEA/409

INTERNATIONAL APPLICATION NO PCT/SG98/00023	INTERNATIONAL FILING DATE 18 MARCH 1998	PRIORITY DATE CLAIMED 18 MARCH 1998

17. [X] The following fees are submitted:

Basic National Fee (37 CFR 1.492(a)(1)-(5):

Neither international preliminary examination fee (37 CFR 1.482)

Nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO (1.492(a)(3)) $970.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO (1.492(a)(5) $840.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO(1.492(a)(2)) $690.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) (1.492(a)(1)) $670.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) . . . . $ 96.00

				CALCULATIONS	PTO USE ONLY
ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 840.00	
Surcharge of $130.00 for furnishing the oath or declaration later than [ ] **20** [ ] **30** months from the earliest claimed priority date (37 C.F.R. 1.492)(e)).				$	
Claims	**Number Filed**	**Number Extra**	**Rate**	$	
Total Claims	45 -20=	25	X $ 18.00	$ 450.00	
Independent Claims	8 -3=	5	X $ 78.00	$ 390.00	
Multiple dependent claim(s) (if applicable)			+ $260.00	$	
TOTAL OF ABOVE CALCULATIONS =				$1680.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$1680.00	
Processing fee of $130.00 for furnishing the English translation later than [ ] **20** [ ] **30** months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$1680.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$1720.00	
				Amt. refunded	$
				charged	$

a. [X] A check in the amount of $1680 & 40 to cover the above fees is enclosed.

b. [ ] Please charge our Deposit Account No. 02-4377 in amount of $___ to cover the above fees. A copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4377. A copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, New York 10112-4498

Signature Paul A. Ragusa

August 17, 2000

Date

38,587

Registration No.

METHOD AND APPARATUS FOR CAMOUFLAGING DATA

Field of the Invention

The present invention relates generally to encoding methods, and more particularly to a method and apparatus for steganographic encoding of data.

The encoding method is espartially suited to digital camouflaging of audio, still image and video data and it will be convenient to describe the method and associated apparatus in relation to that example application. It should be appreciated, however, that the invention is intended for broader application and use. For example, the encoding method of the present invention may also be used in the field of data encryption.

Background of the Invention

The tremendous growth in multimedia products and services provided via the internet has led to the need for copyright authentication and for protecting data integrity. In the past few years, a number of digital watermarking techniques have been developed for the purpose of resolving legal use issues associated with copyright information on the internet.

A number of digital watermarking techniques have recently been patented. Examples of these include US Patent 5,636,292 to Rhoads (1997) and US Patent 5,659,726 to Sandford and Handel (1997). Rhoads discloses methods to impress an identification code on a carrier, such as an electronic data signal or a physical medium, in a manner that permits the identification code to be later discerned and the carrier thereby identified. Sandford and Handel disclose a method of embedding auxiliary information into host data, such as a photograph, television signal, facsimile transmission, or identification card. The method operates by manipulating a noise component of the host data in accordance with the auxiliary information.

Throughout this specification the word "steganography" is intended to denote any of various methods seeking to conceal the existence of a message within some other medium such that any unintended party who intercepts the medium does not know it contains the concealed message and does not therefore obtain the information contained in the message. Digital watermarking is one example of a steganographic method used to embed secondary data, such as text, in primary or host data, such as a digitized image.

The word "cryptography" is intended to denote any of various techniques seeking to hide information contained in a message such that when the message is transmitted from a sender to a receiver any third party intercepting the message cannot read it or extract the information contained in the message.

In the present context, the word "camouflaging" is intended to denote a steganographic encoding method which conceals secondary data by utilizing a combination of primary or host data and key data. The encoding method may not actually embed information in the primary data, as in watermarking, but may utilize information elements existing in the primary data.

Many prior art digital watermarking techniques, including the techniques disclosed in the above US patents, are only able to conceal limited information, such as a few logical bits (ie. "1" and "0") or a few characters (eg. "A12"), in the host data. However, to record detailed ownership information for a host work in which copyright subsists, such as an image of Singapore, an entire message or sentence may need to be concealed in, or associated with, the host data. For example, the sentence "Digital image of Singapore is the property of Mr John Tan, dated 16 December 1997" may provide more conclusive proof as to true ownership of the host work than having to rely on just a simple code to assess copyright infringement.

There therefore remains a need for a steganographic encoding method and apparatus which may allow a relatively long string of secondary data (such as text) to be camouflaged in association with primary data (such as image, audio or video data) whilst producing minimal degradation of the primary or host data. In some embodiments, the primary data may be absolutely unaltered by the encoding process.

Besides the above mentioned application on the internet, many potential consumer, commercial and service applications may benefit from the use of digital camouflaging/watermarking technology, both for copyright protection purposes and for secure transmission of information. These applications include encoding of text containing ownership identification or attribute information associated with digital still or video cameras, copyright protection and royalty tracking of sound recordings in the music industry. Commercial and service sectors may also benefit from secure transmission and reception of sensitive information that could be camouflaged in normal data streams transmitted through an open channel.

Summary of the Invention

In one aspect, the present invention provides a method of steganographic encoding including the steps of:

(A) providing primary data containing a plurality of addressable first data elements;

(B) providing secondary data containing a plurality of second data elements; and

(C) for each second data element:

(C1) searching for a first data element which matches content of the second data element, and

(C2) generating a key element including the address of the matching first data element when a match is found for the content of the second data element.

When a match is found for the content of the second data element, the address of the matching first data element may be stored as a key element associated with the second data element. A string of key elements (containing addresses) may be associated with a corresponding string of second data elements. The string of key elements may specify where in the primary data each second data element of the secondary data is to be found. The secondary data may in this context be considered to be camouflaged in the primary data and the key data. Unique key data which is generated for given primary and secondary data may be stored for use in a complementary decoding method which is described below.

The primary and secondary data may be represented digitally. However, in its broadest aspects, the invention is applicable to any form of data representation or notation using any convenient set of symbols. The primary data may represent a still image, motion video, audio, text or other type of information. Likewise, the secondary data may represent a still image, motion video, audio, text or other information. In a preferred form of the invention, the secondary data includes a text message and each second data element includes an alphanumeric character. The alphanumeric characters may be used to compose the text message.

In a typical application of the invention the text message may include copyright information relating to the image, video, audio, etc. contained in the primary data. In one embodiment, the text message may include one or more of the following: a title, an artist, a copyright holder, a body to which royalties should be paid, and general terms of publisher distribution.

The primary data may include a still image. The first data elements may be arranged in a two-dimensional array wherein each first data element defines a characteristic associated with a still image element. Typically, the first data elements are obtained from a stream of data representing a digitised still image. The image may be obtained from a still digital camera, a computer game or other software, or other source. It may be a greyscale or color image, for example, and may be stored in any known format, eg. BMP, GIF, TIFF, or JPEG.

The primary data may alternatively or additionally include motion video. The first data elements may be arranged in a three-dimensional array wherein each first data element defines a characteristic associated with a motion video element. Typically, the first data elements are obtained from a stream of data representing digitised motion video. The digitised video may be obtained from a Video Compact Disc (VCD) player, a Laser Disc (LD) player, a computer game or other software, a Digital Versatile Disc (DVD) player or other source, and may be stored in any known format, eg. MPEG.

The primary data may alternatively or additionally include audio information. The first data elements may be arranged in a one-dimensional array wherein each first data element defines a characteristic associated with a digital audio sample. Typically, the digital audio samples are obtained from a stream of data representing digitised sound or music. The digitised sound may be obtained from a Compact Disc (CD) player, Digital Audio Tape (DAT) player, Laser Disc player, Video Compact Disc (VCD) player or other source, and may be stored in any known format eg. WAV, AIFF, etc.. In one embodiment, the digital audio samples are obtained from two streams of data representing two channels of digitised sound for stereo reproduction.

In the encoding method described above, the first and second data elements may be represented by integer values and step (C) may further include:

when a match is not found for the content of a second data element;

(C3) producing an adjusted second data element by incrementing or decrementing the integer value of the second data element,

(C4) searching for a first data element which matches the integer value of the adjusted second data element, and

(C5) generating a key element including the address of the matching first data element when a match is found for the adjusted second data element, and replacing the content of the matching first data element with the integer value of the second data element prior to producing the adjusted second data element.

When a match is not found for the adjusted second data element the method may further include:

(C6) producing a new adjusted second data element by incrementing or decrementing the adjusted second data element and repeating steps (C4) and (C5) for the new adjusted second data element.

For example, if a desired integer value, say, 105 is not found in the primary data, a search is conducted to locate values 104 or 106. If one of these values is found, the address of the first data element containing that value is stored in a key element, and the content of the first data element (104 or 106) is replaced with the value 105. If on the other hand the values 104 or 106 are not found, a search is conducted for values 103 or 107. This modification of the primary data may be considered to be a form of embedding of the secondary data in the primary data, in the watermarking sense, but is only performed in the relatively rare event that a desired integer value is not found in the primary data. It has been found that these rarely occurring changes are imperceptible in the modified primary image, video or audio data.

The modified version of the primary data may subsequently be stored for distribution via the internet or other means. The modified primary data contains the secondary data which can be extracted at any future time using the associated key data generated during the encoding process.

The encoding method may include "data shifting" steps prior to step (C). The data shifting steps may be required whenever the range for the secondary data does not fall within the range for the primary data. This may occur for example when the primary data is a digitised audio signal and the secondary data is a text message. Similar data shifting steps may be applied to other types of data. The data shifting steps may include:

determining a range for the contents of the first data elements,

determining a range for the contents of the second data elements,

comparing the range for the first data elements with the range for the second data elements,

shifting the contents of the second data elements when the range for the second data elements falls outside of the range for the first data elements, such that the range for the second data elements falls substantially within the range for the first data elements, and

using the shifted second data elements as the second data elements in step (C).

Preferably, the step of determining a range for the contents of the first data elements includes: calculating a mean and standard deviation for the first data elements; and determining a lower limit for the first data elements based on the mean and standard deviation. The step of determining a range for the contents of the second data elements may include establishing as a reference a minimum value which can be attributed to the range of possible second data elements. The step of comparing may include calculating an offset value by subtracting the reference value from the lower limit, and the step of shifting may include adding the offset value to the contents of each second data element. Preferably the offset value is stored with the key elements in the key data.

It will be appreciated that when a data shifting offset is applied to the secondary data by the encoding method, the complementary decoding method should also include steps to reverse the data shifting offset. The offset value may be retrieved from the key data.

Compared to existing steganographic or watermarking techniques the present invention has the distinct advantage that long sentences of text may be camouflaged. Even with long text strings, the integrity of the primary data is in most cases not affected or compromised. The primary data may remain absolutely unchanged by the encoding method because the method utilises data already present in the primary data. Even in those cases where specific values contained in the secondary data cannot be found in the primary data, and the primary data is modified to insert those values, the primary data may remain substantially unaltered.

In another aspect, the present invention provides a method of steganographic decoding of secondary data including a plurality of second data elements, said secondary data being encoded in key elements in association with primary data, said method including the steps of:

(A) providing said primary data containing a plurality of addressable first data elements;

(B) providing said key elements, each key element including an address of a first data element; and

(C) for each key element, generating a said second data element by extracting the content of the addressed first data element.

In a further aspect, the present invention provides an apparatus for steganographic encoding including:

(A) means for providing primary data containing a plurality of addressable first data elements;

(B) means for providing secondary data containing a plurality of second data elements;

(C) means for searching, for each second data element, a first data element which matches content of the second data element, and

(D) means for generating a key element including the address of the matching first data element when a match is found for the content of the second data element.

In a still further aspect, the present invention provides an apparatus for steganographic decoding of secondary data including a plurality of second data elements, said secondary data being encoded in key elements in association with primary data, said apparatus including:

(A) means for providing said primary data containing a plurality of addressable first data elements;

(B) means for providing said key elements, each key element including an address of a first data element; and

(C) means for generating a second data element for each key element by extracting the content of the addressed first data element.

In a still further aspect of the present invention the method of encoding described above may be applied to cryptography. In applications involving cryptographic encoding a hidden message may be transmitted from a sender to a receiver. The message may be encoded in the key elements which are generated by the method in association with the primary data. The message to be hidden in this case corresponds to the second data elements. The hidden message may be decoded by the receiver from the key elements by utilizing the primary data in a complementary decoding method.

Brief Description of the Drawings

The accompanying drawings, which are incorporated into and constitute part of the description of the invention, illustrate embodiments of the invention and serve to explain the principles thereof. It is to be understood, however, that the drawings and following detailed description are given for the purposes of illustration only and are not intended as a definition of the limits of the invention.

In the drawings:

Figure 1A illustrates a one dimensional data array containing integer values representing a digitised audio signal;

Figure 1B illustrates a two dimensional data array containing integer values representing a digital still image;

Figure 2 illustrates an example of an audio signal;

Figure 3 illustrates an example of a digital image;

Figure 4 illustrates a table of the ASCII character set;

Figure 5 illustrates a typical greyscale histogram for a digital image;

Figures 6A and 6B illustrate a two dimensional data array of 4 x 8 data elements representing pixels of a greyscale image;

Figure 7 is a schematic block diagram of a digital camouflaging apparatus according to the present invention;

Figure 8 is a pseudocode of the digital camouflaging text encoder;

Figure 9 is a pseudocode of the digital camouflaging text decoder;

Figure 10 is a pseudocode of the spatial location program used in the encoding process shown in Figure 8;

Figure 11 illustrates an example of digital camouflaging of an alphanumeric text message in an image; and

Figure 12 illustrates an entire English text paragraph which is camouflaged in the image of Figure 11.

Description of Preferred Embodiments

In a preferred embodiment of the present invention, involving digital camouflaging, the invention exploits the data values present in various digital formats, such as for audio, image and video, for encoding and decoding of alphanumeric character strings.

Figure 1A illustrates a one dimensional data array containing integer values which may, for example, represent a digital audio signal (speech or music) sampled under a conventional digital sound format.

Figure 1B illustrates a two dimensional data array containing integer values which may, for example, represent a digital still image in GIF or JPEG format, or a video frame in MPEG format.

Figure 2 illustrates a typical digital sampled audio waveform (music) in WAV format, with amplitude (vertical axis) plotted against time (horizontal axis).

Figure 3 illustrates a typical 8 bit greyscale image of 512 x 512 pixels.

Digital camouflaging may be described as analogous to natural camouflaging, where the camouflaged object (for example a leaf, insect or reptile) conceals itself completely into the surrounding environment. In the present invention, digital camouflaging conceals secondary data, such as an alphanumeric text string in integer form, in primary data, such as an image, by locating the spatial positions of integer values that match the text string values.

Figure 4 illustrates a table of the ASCII character set. The digits at the left of the table are the left digits of the decimal equivalent (0 - 127) of the character code, and the digits at the top of the table are the right digits of the character code. For example, the character code for "F" is 70, and the character code for "&" is 38. The commonly used alphanumeric codes for text strings are as follows:

48 to 57 represent the numeric values "0 - 9",
65 to 90 represent the upper case alphabet "A - Z", and
97 to 122 represent the lower case alphabet "a - z".

The present invention may be applied to many different data formats for audio, image and video data. In the case of digital image and video camouflaging, a histogram distribution for most natural images, such as human faces or landscapes, would span a wide range of greyscale levels. For example, an 8 - bit or 256 grey level image would contain image pixel values between 0 and 255. Figure 5 illustrates a typical image histogram. It can be seen that a wide spread of pixel values is available in the image for exact matching to alphanumeric character codes to be camouflaged. It can also be seen that a large number of pixels at different spatial locations within the image have the same integer value. For example, the value 105 appears in approximately 2500 pixels in the image.

For each alphanumeric character of a text string to be encoded in an image, a search for an exact matching of this character to an image pixel is first performed. Once the pixel value is found, the address of the spatial location of the pixel is stored in a key element. However, more than one pixel containing the same value as the alphanumeric character value is likely to arise. When this occurs, the encoding method will preferably select the first pixel that it finds. The address of this pixel will form an important part of key data that will later be used to decode the camouflaged alphanumeric character text string. Table 1 gives an example of an alphanumeric text string "This is an Example" and the corresponding integer values.

TABLE 1

Alphanumeric Character	Integer Value
T	84
h	104
i	105
s	115
space	32
i	105
s	115
space	32
a	97
n	110
space	32
E	69
x	120
a	97
m	109
p	112
l	108
e	101

Thus, "This is an Example" is equivalent to the data array [84 104 105 115 32 105 115 32 97 110 32 69 120 97 109 112 108 101].

Figures 6A and 6B show an example of a two-dimensional data array representing pixel values of a 4 x 8 pixel image. The terms (1, 1), (1, 2), ... (4, 8) are spatial location addresses of the pixels in the image. These addresses are stored as key elements when the alphanumeric character values are matched to pixel values during searching. For example, in the encoding process, the first alphanumeric character "T" with its integer value of 84 (shown in bold in Figure 6A) would match the values of pixels located at (3,1) and (2, 8). The address of the first location (3, 1) will be stored in a corresponding key element for later use in the complementary decoding process.

There are some instances, however, where after searching through all the pixel values in an image, a particular alphanumeric character value does not result in an exact match to its value. In these instances, the present invention will perform a new search for an adjusted value that is one pixel off either side of the character value. The address of the pixel containing the adjusted value is then stored as the key element. For example, if the first alphanumeric character of the text string is a "T", with an integer value of 84, when the search of the pixel values does not locate a single value of 84, a new search would commence to locate values 83 or 85. These values correspond to alphanumeric characters of "S" and "U", respectively.

In one embodiment, when the new search locates a pixel having a value of 83 or 85 it will first check whether that pixel has already been used. If so, and providing that the same pixel values occur at other addresses, the encoding method will select another pixel having the value of 83 or 85. Once such a pixel has been found, the pixel value is overwritten with the character value of 84.

If the adjusted value, being one pixel value off either side of the character value, cannot be found, then a second search commences to locate a pixel value having a new adjusted value, of 2 pixel values off either side of the character value (ie. 82 and 86 in the present example). The matching and overwriting steps are then repeated as before.

Referred to Figure 6B, and using the same example of alphanumeric text and image pixel values as in Figure 6A, the third and sixth alphanumeric characters "i", which correspond to the value 105, will not find an exact match after searching the (4 x 8) image, as there is no such value existing. In this case, the encoding method will search for a value that is an increment or decrement to that value.

The method steps involved in "off-pixel" searching and overwriting are as follows:

1. Search for character value of 105 ("i") in image.
2. None found.
3. Increment or decrement value to 104 or 106.
4. None found for 106.
5. Two pixels found having value 104 (shown in bold in Figure 6B).
6. Check whether pixel has been used previously.
7. If yes, store second pixel spatial location address; overwrite pixel value in image with character value 105.
8. If no, store first pixel spatial location address; overwrite pixel value in image with character value 105.

Most natural images contain pixel values spanning over a wide range, thus allowing almost all alphanumeric character values to be exactly matched. After many tests with different natural images it has been found that the maximum number of off-pixel searches required is generally less than ± 3 pixel values. Correlation analysis preformed on the same image before and after data camouflaging using the present invention indicates that the images are often exactly identical. Even when there is no exact match of the pixel values to the alphanumeric character values, the minute change caused by overwriting just a few pixels in the image, for example from 104 to 105, has an insignificant degrading affect on image quality. Under these conditions, the correlation coefficient between the two images still results, for all practical cases, in a value of substantially one.

The complementary decoding process is relatively straight forward as it uses the unique key data generated from the spatial location addresses of pixels that match the alphanumeric characters composing the text string. The unique key data provides the addresses of the spatial locations from which the camouflaged text string may be extracted from the image.

The key data is unique to a specific text string and specific image. If the key data is applied to another image, the text string extracted will be just a random sequence of characters.

For digital audio camouflaging, the dynamic range of values of audio samples associated with music or speech may not be as wide as in the case for digital still/video images. The audio integer values may also be in a range that is somewhat different to the range of alphanumeric character values. A slightly different approach is therefore needed for camouflaging of alphanumeric text strings in digital audio data.

The present invention may accordingly include an adaptive statistical approach to first determine the dynamic range of the audio samples. The mean (μ) and the standard deviation (σ) of the audio samples are determined and used to calculate a lower limit of the audio samples. For example, using the alphanumeric character code for “A”, which corresponds to an integer value of 65, as a reference, the alphanumeric character set may be adaptively shifted to coincide with the dynamic range of the audio samples. This adaptive statistical approach has proven very robust for embedding alphanumeric text strings into digital audio samples of music and speech. The method steps involved in the adaptive statistical range shifting process are preferably as follows:

<u>Encoding</u>

1. Store integer value of alphanumeric reference character, eg. 65 for “A”.
2. Determine mean and standard deviation of audio samples.
3. Calculate lower limit of audio sample range, eg. by subtracting three times the standard deviation from the mean (ie. μ - 3σ).
4. Obtain “data shifting offset” by subtracting reference character value from the lower limit of the audio sample range.
5. Add data shifting offset to each alphanumeric character.
6. Perform search, key element generation and overwriting steps as described above in relation to image example.
7. Generate unique key data from key elements.

Decoding

8. Extract audio sample values based on locations addressed in key elements of unique key data.

9. Reverse data shifting process, by subtracting data shifting offset from values extracted, to obtain alphanumeric character values.

Referring now to Figure 7, there is shown a schematic block diagram of a digital encoding/decoding apparatus according to an embodiment of the present invention. Data samples 10 are encoded with an alphanumeric character string 12 through a data encoding means 14. Encoded data samples 16 and unique key data 18, containing spatial location addresses, are obtained from the data encoding means 14. These two outputs 16, 18 are used in the reverse decoding means 20. The original alphanumeric character string 12 is extracted as 12A from the encoded data samples 16 using the location address contained in the unique key data 18. The encoded data samples 16 remain unchanged or minimally changed as 16A by the decoding means 20.

A pseudocode of the digital camouflaging text encoder is shown in Figure 8 and a pseudocode of the digital camouflaging text decoder is shown in Figure 9. A pseudocode of the spatial location program used in the encoding process is shown in Figure 10. In these figures the term "unlabelled" is used to refer to the original data and the term "labelled" is used to refer to the encoded data.

An example of the use of the present invention for camouflaging text labels in a digital image is illustrated in Figure 11. A text string containing 83 characters "This example shows an alphanumeric text message camouflaged into the image of Lena." is camouflaged in the Lena image. The correlation coefficient equals exactly one, indicating that there is no difference between the labelled and unlabelled images. Moreover, an entire paragraph of English text containing 126 words and 784 characters, as shown in Figure 12, is camouflaged in the same Lena image and, once again, the correlation coefficient is equal to exactly one.

The present invention of camouflaging alphanumeric character text strings into digital data has many potential applications for resolving copyright protection issues in the consumer sector or for secure transmission of messages in the commercial and service sectors. For example, data camouflaging may be incorporated into consumer electronic products, such as digital still/video cameras and, more recently, VCD and DVD players, to authenticate the true ownership of intellectual property rights or product ownership. Another major consumer area for data camouflaging is that of preventing illegal copying and downloading of satellite images, music CD's, and tapes.

In the commercial sector, copyright protection of multimedia data on the Internet needs also to be monitored closely, as there is a tremendous amount of original data, in the form of music, image and video, illegally downloaded and redistributed without the consent of the true owners. The present invention can be used to address this problem, as well as providing for the secure transmission of messages in commercial and other operations. Similarly, in the service sector such as security and banking, secret text messages can be camouflaged in an ordinary image or speech for secure transmission.

Those skilled in the art would appreciate that various adaptations and modifications of the just described preferred embodiments may be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.

CLAIMS

1. A method of steganographic encoding including the steps of:

(A) providing primary data containing a plurality of addressable first data elements;

(B) providing secondary data containing a plurality of second data elements; and

(C) for each second data element:

(C1) searching for a first data element which matches content of the second data element, and

(C2) generating a key element including the address of the matching first data element when a match is found for the content of the second data element.

2. A method of steganographic encoding as defined in claim 1 wherein the first and second data elements are represented by integer values and wherein step (C) further includes:

when a match is not found for the content of a second data element;

(C3) producing an adjusted second data element by incrementing or decrementing the integer value of the second data element,

(C4) searching for a first data element which matches the integer value of the adjusted second data element, and

(C5) generating a key element including the address of the matching first data element when a match is found for the adjusted second data element, and replacing the content of the matching first data element with the integer value of the second data element prior to producing the adjusted second data element.

3. A method of steganographic encoding as defined in claim 2 wherein step (C) further includes:

when a match is not found for the content of the adjusted second data element;

(C6) producing a new adjusted second data element by incrementing or decrementing the adjusted second data element and repeating steps (C4) and (C5) for the new adjusted second data element.

4. A method of steganographic encoding as defined in claim 1 wherein, prior to step (C) the method includes:

determining a range for the contents of the first data elements,

determining a range for the contents of the second data elements,

comparing the range for the first data elements with the range for the second data elements,

shifting the contents of the second data elements when the range for the second data elements falls outside of the range for the first data elements, such that the range for the second data elements falls substantially within the range for the first data elements, and

using the shifted second data elements as the second data elements in step (C).

5. A method of steganographic encoding as defined in claim 4 wherein the step of determining a range for the contents of the first data elements includes:

calculating a mean and standard deviation for the first data elements; and

determining a lower limit for the first data elements based on the mean and standard deviation.

6. A method of steganographic encoding as defined in claim 4 wherein the step of determining a range for the contents of the second data elements includes:

establishing as a reference a minimum value which can be attributed to the range of possible second data elements.

7. A method of steganographic encoding as defined in claim 6 wherein the

step of comparing includes calculating an offset value by subtracting the reference value from the lower limit.

8. A method of steganographic encoding as defined in claim 7 wherein the step of shifting includes adding the offset value to the contents of each second data element.

9. A method of steganographic encoding as defined in claim 1, further including storing the key elements.

10. A method of steganographic encoding as defined in claim 7 further including storing the offset value with the key elements.

11. A method of steganographic encoding as defined in claim 1 wherein:

step (A) includes providing a digital representation of the content of each first data element,

step (B) includes providing a digital representation of the content of each second data element, and

step (C1) includes comparing values of the digital representations of the first and second data elements.

12. A method of steganographic encoding as defined in claim 1 wherein the secondary data includes a text message and each second data element includes an alphanumeric character.

13. A method of steganographic encoding as defined in claim 12 wherein the text message includes one or more of the following:

a title,

an artist,

a copyright holder,

a body to which royalties should be paid, and general terms for publisher distribution.

14. A method of steganographic encoding as defined in claim 2 further including storing the primary data or modified primary data produced by step (C5).

15. A method of steganographic encoding as defined in claim 1 wherein the primary data includes first data elements arranged in a two-dimensional array wherein each first data element defines a characteristic associated with a still image element.

16. A method of steganographic encoding as defined in claim 15 wherein the first data elements are obtained from a stream of data representing a digitised still image.

17. A method of steganographic encoding as defined in claim 16 wherein the digitised still image is obtained from a still digital camera.

18. A method of steganographic encoding as defined in claim 16 wherein the digitised still image is obtained from a computer game or other software.

19. A method of steganographic encoding as defined in claim 1 wherein the primary data includes first data elements arranged in a three-dimensional array wherein each first data element defines a characteristic associated with a motion video element.

20. A method of steganographic encoding as defined in claim 19 wherein the first data elements are obtained from a stream of data representing digitised motion video.

21. A method of steganographic encoding as defined in claim 20 wherein the digitised video is obtained from a Video Compact Disc player.

22. A method of steganographic encoding as defined in claim 20 wherein the digitised video is obtained from a Laser Disc player.

23. A method of steganographic encoding as defined in claim 20 wherein the digitised video is obtained from a digitised movie contained within a computer game or other software.

24. A method of steganographic encoding as defined in claim 20 wherein the digitised video is obtained from a Digital Versatile Disc player.

25. A method of steganographic encoding as defined in claim 1 wherein the primary data includes first data elements arranged in a one-dimensional array wherein each first data element defines a characteristic associated with a digital audio sample.

26. A method of steganographic encoding as defined in claim 25 wherein the digital audio samples are obtained from a stream of data representing digitised sound or music.

27. A method of steganographic encoding as defined in claim 25 wherein the digital audio samples are obtained from two streams of data representing two channels of digitised sound for stereo reproduction.

28. A method of steganographic encoding as defined in claim 25 wherein the digitised sound or music is obtained from a Compact Disc player.

29. A method of steganographic encoding as defined in claim 25 wherein the digitised sound or music is obtained from a Digital Audio Tape player.

30. A method of steganographic encoding as defined in claim 25 wherein the

digitised sound or music is obtained from a Laser Disc player.

31. A method of steganographic encoding as defined in claim 25 wherein the digitised sound or music is obtained from a Video Compact Disc player.

32. A method of steganographic encoding as defined in claim 1 wherein the number of first data elements is greater than the number of second data elements.

33. A method of steganographic encoding as defined in claim 1 wherein the address of each first data element is used only once for generating the key elements, whereby second data elements having equal contents are matched to first data elements having different addresses.

34. A method of steganographic decoding of secondary data including a plurality of second data elements, said secondary data being encoded in key elements in association with primary data, said method including the steps of:

(A) providing said primary data containing a plurality of addressable first data elements;

(B) providing said key elements, each key element including an address of a first data element; and

(C) for each key element, generating a said second data element by extracting the content of the addressed first data element.

35. A method of steganographic decoding as defined in claim 34 wherein the contents of the second data elements are shifted by an offset value further including:

(D) providing said offset value, and

(E) subtracting the offset value from the contents of the second data elements.

36. A method of steganographic decoding as defined in claim 34 wherein each second data element includes an alphanumeric character.

37. An apparatus for steganographic encoding including:

(A) means for providing primary data containing a plurality of addressable first data elements;

(B) means for providing secondary data containing a plurality of second data elements;

(C) means for searching, for each second data element, a first data element which matches content of the second data element, and

(D) means for generating a key element including the address of the matching first data element when a match is found for the content of the second data element.

38. An apparatus for steganographic encoding as defined in claim 37 wherein the first and second data elements are represented by integer values, said apparatus further including:

(E) means for producing an adjusted second data element by incrementing or decrementing the integer value of the second data element when a match is not found for the content of a secondary data element,

(F) means for searching for a first data element which matches the integer value of the adjusted second data element,

(G) means for generating a key element including the address of the matching first data element when a match is found for the adjusted second data element, and

(H) means for replacing the content of the matching first data element with the integer value of the second data element prior to producing the adjusted second data element.

39. An apparatus for steganographic encoding as defined in claim 37 further including, means for producing a new adjusted data element by incrementing or

decrementing the adjusted second data element when a match is not found for the adjusted second data element.

40. An apparatus for steganographic encoding as defined in claim 37 further including:

means for determining a range for the contents of the first data elements,

means for determining a range for the contents of the second data elements,

means for comparing the range for the first data elements with the range for the second data elements,

means for shifting the contents of the second data elements when the range for the second data elements falls outside of the range for the first data elements, such that the range for the second data elements falls substantially within the range for the first data elements, and

means for using the shifted second data elements as the second data elements.

41. An apparatus for steganographic decoding of secondary data including a plurality of second data elements, said secondary data being encoded in key elements in association with primary data, said apparatus including:

(A) means for providing said primary data containing a plurality of addressable first data elements;

(B) means for providing said key elements, each key element including an address of a first data element; and

(C) means for generating a second data element for each key element by extracting the content of the addressed first data element.

42. A method of cryptographic encoding including the steps of:

(A) providing primary data containing a plurality of addressable first data elements;

(B) providing secondary data containing a plurality of second data elements; and

(C) for each second data element:

(C1) searching for a first data element which matches content of the second data element, and

(C2) generating a key element including the address of the matching first data element when a match is found for the content of the second data element.

43. A method of cryptographic decoding of secondary data including a plurality of second data elements, said secondary data being encoded in key elements in association with primary data, said method including the steps of:

(A) providing said primary data containing a plurality of addressable first data elements;

(B) providing said key elements, each key element including an address of a first data element; and

(C) for each key element, generating a second data element by extracting the content of the addressed first data element.

44. An apparatus for cryptographic encoding including:

(A) means for providing primary data containing a plurality of addressable first data elements;

(B) means for providing secondary data containing a plurality of second data elements;

(C) means for searching for each second data element a first data element which matches content of the second data element, and

(D) means for generating a key element including the address of the matching first data element when a match is found for the content of the second data element.

45. An apparatus for cryptographic decoding of secondary data including a plurality of second data elements, said secondary data being encoded in key

elements in association with primary data, said apparatus including:

(A) means for providing said primary data containing a plurality of addressable first data elements;

(B) means for providing said key elements, each key element including an address of a first data element; and

(C) means for generating a second data element for each key element by extracting the content of the addressed first data element.

Fig 1A

[100 120 90 80 102 88 55 16]

Fig 1B

130	150	200	255	100	56	10	12
120	200	111	201	178	77	30	11
189	176	100	211	189	17	20	13
120	200	111	201	178	79	30	11
185	106	130	241	189	97	20	19
119	186	120	231	189	21	60	43
120	200	111	201	178	79	30	11
185	106	130	241	189	97	20	19

Fig 2

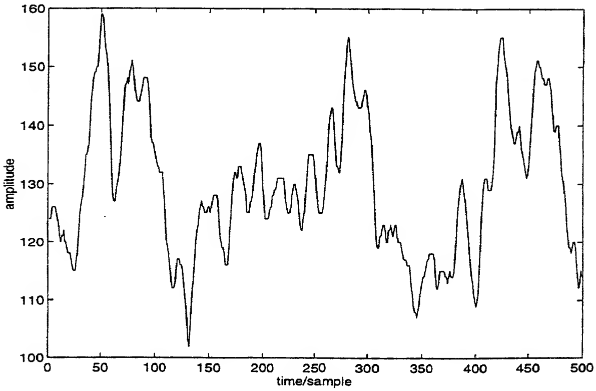


Figure 3

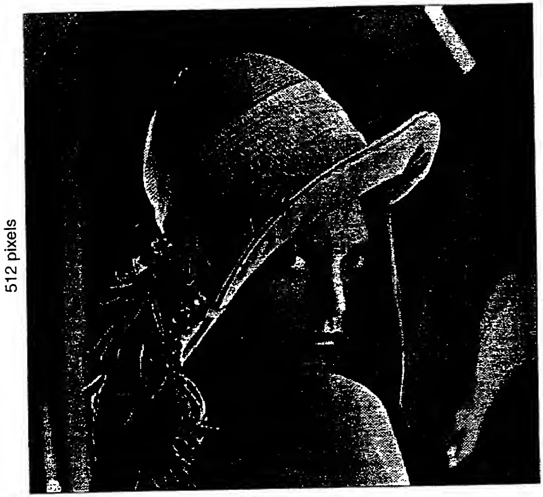


Fig 4

ASCII Character Set

	0	1	2	3	4	5	6	7	8	9
0	nul	soh	stx	etx	eot	enq	ack	bel	bs	ht
1	nl	vt	ff	cr	so	si	dle	dc1	dc2	dc3
2	dc4	nak	syn	etb	can	em	sub	esc	fs	gs
3	rs	us	sp	!	"	#	$	%	&	'
4	(	)	*	+	,	-	.	/	0	1
5	2	3	4	5	6	7	8	9	:	;
6	<	=	>	?	@	A	B	C	D	E
7	F	G	H	I	J	K	L	M	N	O
8	P	Q	R	S	T	U	V	W	X	Y
9	Z	[	\	]	^	_	`	a	b	c
10	d	e	f	g	h	i	j	k	l	m
11	n	o	p	q	r	s	t	u	v	w
12	x	y	z	{	|	}	~	del		

Fig 5

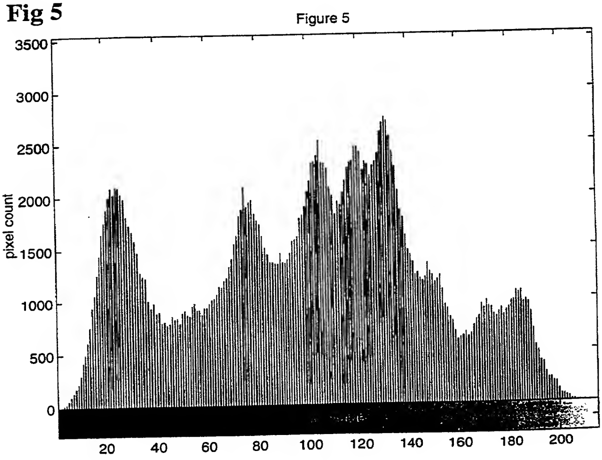


Fig 6A

	(1,1)	(2,1)	(3,1)	(4,1)
(1,1)	100	110	**84**	192
(1,2)	120	65	78	103
(1,3)	115	20	144	76
(1,4)	90	78	46	104
(1,5)	104	89	120	42
(1,6)	99	72	122	88
(1,7)	78	120	69	77
(1,8)	40	**84**	65	10

Fig 6B

	(1,1)	(2,1)	(3,1)	(4,1)
(1,1)	100	110	84	192
(1,2)	120	65	78	103
(1,3)	115	20	144	76
(1,4)	90	78	46	**104**
(1,5)	**104**	89	120	42
(1,6)	99	72	122	88
(1,7)	78	120	69	77
(1,8)	40	84	65	10

Fig 7

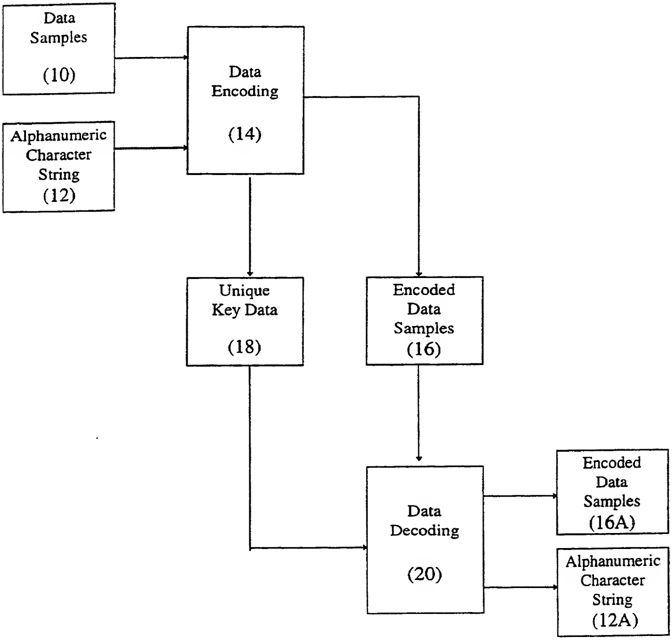

Data Samples (10)
Alphanumeric Character String (12)
Data Encoding (14)
Unique Key Data (18)
Encoded Data Samples (16)
Data Decoding (20)
Encoded Data Samples (16A)
Alphanumeric Character String (12A)

Fig 8

```
PROCEDURE TEXT ENCODER

        READ UNLABELLED DATA;
        CONVERT UNLABELLED DATA INTO INTEGER ARRAY
        READ ALPHANUMERIC CHARACTER STRING;
        CONVERT CHARACTER STRING TO INTEGER ARRAY;

        PROCEDURE SPATIAL LABELLER;

        GENERATE UNIQUE KEY DATA FROM KEY ELEMENTS CONTAINING
        MATCHING LOCATIONS;
        CONVERT LABELLED INTEGER ARRAY TO LABELLED DATA;
        STORE UNIQUE KEY;
        STORE LABELLED DATA

END
```

Fig 9

```
PROCEDURE TEXT DECODER

        READ LABELLED DATA;
        CONVERT LABELLED DATA INTO INTEGER ARRAY;

        READ UNIQUE KEY;
        EXTRACT SPATIAL LOCATIONS FROM UNIQUE KEY;
        DECODE CHARACTER INTEGER ARRAY FROM SPATIAL LOCATIONS;
        CONVERT CHARACTER INTEGER ARRAY TO ALPHANUMERIC
        CHARACTER STRING;
        DISPLAY ALPHANUMERIC CHARACTER STRING

END
```

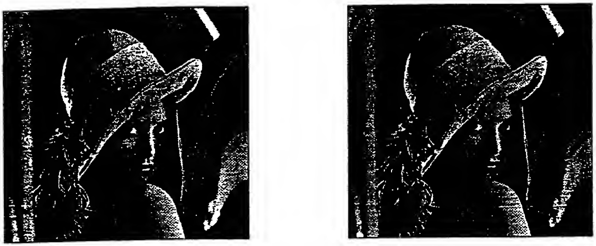
Fig 10

```
PROCEDURE SPATIAL LABELLER

        READ UNLABELLED DATA INTEGER ARRAY;
        READ CHARACTER INTEGER ARRAY;
        DETERMINE LENGTH OF CHARACTER INTEGER ARRAY;
        DO 1 TO LENGTH
                SEARCH AND MATCH UNLABELLED DATA ELEMENT AND
                CHARACTER ELEMENTS;
                IF NO MATCH THEN
                        INCREMENT OR DECREMENT CHARACTER INTEGER
                        VALUE BY ONE;
                        REPEAT SEARCH;
                                OVERWRITE UNLABELLED DATA INTEGER WITH
                                VALUE TO BE MATCHED;
                                STORE SPATIAL LOCATION TO KEY ELEMENT;
                        UNTIL DATA ELEMENT MATCHED
                ELSE
                        STORE SPATIAL LOCATION TO KEY ELEMENT;
                END
                STORE LABELLED DATA ELEMENT TO LABELLED INTEGER
                ARRAY;
        END

END
```

Fig 11



Unlabeled:lena512

labeled:lena512

Fig 12

“As digital watermarking is a relatively new technology, DataMark expects the market for its product DataCam to be substantial. For example, in a recent survey on the Internet market, compound annual growth rates of 37.6% and 91.1% in Internet access and software products, respectively, are forecast for the years from 1996 to 2000. These growth rates translate to revenues of US$3.15b for 1996 and $11.3b for 2000, in Internet access, and $916m for 1996 and $12.2b for 2000, in software products [1]. As the Internet continues to grow on a rapid scale, more legal questions related to copyright protection will surface and need to be seriously addressed by the Internet community. One potential solution is the use of digital watermarking or camouflaging technology in digital data. ”

BAKER BOTTS L.L.P.
FILE NO.: A33361-PCT-USA

COMBINED DECLARATION AND POWER OF ATTORNEY

(Original, Design, National Stage of PCT, Divisional, Continuation or C-I-P Application)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND APPARATUS FOR CAMOUFLAGING DATA

This declaration is of the following type:

[]original
[] design
[X] national stage of PCT.
[] divisional
[] continuation
[] continuation-in-part (C-I-P)

the specification of which: *(complete (a), (b), or (c))*

(a) [ ] is attached hereto.
(b) [ ] was filed on as Application Serial No. and was amended on *(if applicable).*
(c) [x] was described and claimed in PCT International Application No. PCT/SG98/00023 filed on March 18, 1998 and was amended on *(if applicable).*

Acknowledgement of Review of Papers and Duty of Candor

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of the subject matter claimed in this application in accordance with Title 37, Code of Federal Regulations § 1.56.

[ ] In compliance with this duty there is attached an information disclosure statement. 37 CFR 1.98.

Priority Claim

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT International Application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT International Application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application on which priority is claimed

(complete (d) or (e))

(d) [ ] no such applications have been filed.
(e) [X] such applications have been filed as follows:

NY02:273703.1

that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

1-0

FULL NAME OF SOLE OR FIRST INVENTOR	LAST NAME HO	FIRST NAME ANTHONY	MIDDLE NAME TUNG SHUEN	
RESIDENCE & CITIZENSHIP	CITY Singapore	STATE or FOREIGN COUNTRY Singapore	COUNTRY OF CITIZENSHIP SINGAPORE	
POST OFFICE ADDRESS	POST OFFICE ADDRESS c/o Nanyang Technological University, School of Electrical & Electronic Engineering, Block S2, Nanyang Avenue,	CITY SINGAPORE	STATE or COUNTRY SINGAPORE	ZIP CODE 639 798
DATE 8 August 2000	SIGNATURE OF INVENTOR			
FULL NAME OF SECOND JOINT INVENTOR, IF ANY	LAST NAME	FIRST NAME	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY	STATE or FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE or COUNTRY	ZIP CODE
DATE	SIGNATURE OF INVENTOR			
FULL NAME OF THIRD JOINT INVENTOR, IF ANY	LAST NAME	FIRST NAME	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY	STATE or FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE or COUNTRY	ZIP CODE
DATE	SIGNATURE OF INVENTOR			
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	LAST NAME	FIRST NAME	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY	STATE or FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE or COUNTRY	ZIP CODE
DATE	SIGNATURE OF INVENTOR			
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	LAST NAME	FIRST NAME	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY	STATE or FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE or COUNTRY	ZIP CODE
DATE	SIGNATURE OF INVENTOR			
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	LAST NAME	FIRST NAME	MIDDLE NAME	
RESIDENCE & CITIZENSHIP	CITY	STATE or FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE or COUNTRY	ZIP CODE

PRIOR FOREIGN/PCT APPLICATION(S) FILED WITHIN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO SAID APPLICATION				
COUNTRY	APPLICATION NO.	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 USC 119
				[ ] YES NO [ ]
				[ ] YES NO [ ]
				[ ] YES NO [ ]
ALL FOREIGN APPLICATION[S], IF ANY, FILED MORE THAN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO SAID APPLICATION				
				[ ] YES NO [ ]
				[ ] YES NO [ ]
				[ ] YES NO [ ]

Claim for Benefit of Prior U.S. Provisional Application(s)

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

Provisional Application Number	Filing Date

Claim for Benefit of Earlier U.S./PCT Application(s) under 35 U.S.C. 120

(complete this part only if this is a divisional, continuation or C-I-P application)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior application(s) in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose information as defined in Title 37, Code of Federal Regulations, § 1.56 which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application:

(Application Serial No.) (Filing Date) (Status) (patented, pending, abandoned)

(Application Serial No.) (Filing Date) (Status) (patented, pending, abandoned)

Power of Attorney

As a named inventor, I hereby appoint Dana M. Raymond, Reg. No. 18,540; Frederick C. Carver, Reg. No. 17,021; Francis J. Hone, Reg. No. 18,662; Joseph D. Garon, Reg. No. 20,420; Arthur S. Tenser, Reg. No. 18,839; Ronald B. Hildreth, Reg. No. 19,498; Thomas R. Nesbitt, Jr., Reg. No. 22,075; Robert Neuner, Reg. No. 24,316; Richard G. Berkley, Reg. No. 25,465; Richard S. Clark, Reg. No. 26,154; Bradley B. Geist, Reg. No. 27,551; James J. Maune, Reg. No. 26,946; John D. Murnane, Reg. No. 29,836; Henry Tang, Reg. No. 29,705; Robert C. Scheinfeld, Reg. No. 31,300; John A. Fogarty, Jr., Reg. No. 22,348; Louis S. Sorell, Reg. No. 32,439; Rochelle K. Seide Reg. No. 32,300; Gary M. Butter, Reg. No. 33,841; Marta E. Delsignore, Reg. No. 32,689; and Lisa B. Kole, Reg. No. 35,225 of the firm of BAKER BOTTS L.L.P., with offices at 30 Rockefeller Plaza, New York, New York 10112, as attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith

SEND CORRESPONDENCE TO:	DIRECT TELEPHONE CALLS TO:
BAKER BOTTS L.L.P. 30 ROCKEFELLER PLAZA, NEW YORK, N.Y. 10112 CUSTOMER NUMBER: 21003	BAKER BOTTS L.L.P. (212) 705-5000

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge